DTS
DEPARTMENT OF TECHNOLOGY SERVICES

TECHNICAL ARCHITECTURE REVIEW

Project Name:	**Logging, Log Management, and Monitoring**
Requestor:	Kevin Van Ausdal
Date of Initial Request:	November 19, 2007
Request Description:	As part of its agreement to share tax information with the Tax Commission, the IRS requires compliance with Publication 1075. This publication defines security standards that include logging of all access to systems that store federal tax data, both by administrators and/or users at the OS level as well as access to the actual data. Through the combination of implementing GenTax, moving to secure file transfer from tape as the method of receiving data, and a recent IRS safeguard review, DTS-Tax staff have recognized the lack of required logging capabilities. What enterprise logging resources are available?
Agency or Agencies:	Tax, Enterprise
Reviewers:	Bob Woolley and Dave Fletcher
ARB Acceptance Date:	
Agency Requestor Acceptance Date:	

Introduction and Background

A log is a record of the events occurring within State systems and networks. Logs are composed of log entries. Entries contain information related to a specific event that has occurred within a system or network. Many logs within the State contain records related to computer security. These computer security logs are generated by many sources, including security software, such as antivirus software, firewalls, and intrusion detection and prevention systems; operating systems on servers, workstations, and networking equipment; and, applications.

The number, volume, and variety of computer security logs has increased, which, in turn, has created the need for computer security log management. Log management is the process of generating, transmitting, storing, analyzing, and disposing of computer security log data. Log management is essential to

ensuring that computer security records are stored in sufficient detail for an appropriate period of time. Log analysis is beneficial for identifying security incidents, policy violations, fraudulent activity, and operational problems. Logs support auditing and forensic analysis, internal investigations, and identification of operational trends and long-term problems.

The State is required to store and analyze logs to comply with federal legislation and regulations, including the *Federal Information Security Management Act of 2002* (FISMA), the *Health Insurance Portability and Accountability Act of 1996* (HIPAA), *IRS Security* (Publication 1075), and the *Payment Card Industry Data Security Standard* (PCI DSS), to name a few. In addition, the State is also impacted by other commercial security requirements such as the *Sarbanes-Oxley Act of 2002* (SOX).

Log management at the State requires balancing a limited quantity of log management resources with a continuous supply of log data. Log generation and storage can be complicated by high numbers of log sources; inconsistent log content, formats, and timestamps among sources; and, increasingly large volumes of log data.

Log management involves protecting the confidentiality, integrity, and availability of logs. Log management needs to ensure that security, system, and network administrators regularly perform effective analysis of log data.

The National Institute of Standards and Technology (NIST)[1] has made five core recommendations for effective log management. Organizations should:

- establish policies and procedures for log management;
- prioritize log management appropriately throughout the organization;
- create and maintain a log management infrastructure;
- provide proper support for all staff with log management responsibility; and,
- establish standard log management operational processes.

With these recommendations as a best practice foundation, how is the State of Utah handling log management responsibility? This review addresses these issues from an architecture and operational perspective.

Objectives and Scope of Review

The purpose of this review is to assess the current state of centralized logging services in the context of specific logging requirements by the Utah Tax

[1] Kent, Karen, and Murugiah Souppaya, *Guide to Computer Security Log Management*, NIST Special Publication 800-92, September 2006.

Commission. The report assesses current capabilities, market trends, and makes recommendations for growing a responsive and capable enterprise logging service with the DTS Security office. Cost analysis is limited, since solution alternatives for upgrading the existing requirement have not been firmly established. Documents written for the initial rollout of centralized logging services have been reviewed to gain a sense of the intended scope and vision for centralized logging.

Baseline of Current Architecture

Log management infrastructure typically includes the following three architectural tiers:

- **Log Generation**—Tier 1 includes the hosts that generate log data. Some servers generate log data and use the network to move the data to logging servers. Other systems make data available through other means. Log data is stored using Tier 2 resources and infrastructure.

- **Log Analysis and Storage**—Tier 2 includes log servers that receive log data from Tier 1. Data is typically transferred to the logging server in real time or using some defined batch methodology. Log data can be stored on log or database servers.

- **Log Monitoring**—Tier 3 contains consoles that may be used to monitor and review log data from Tier 2 and provide some level of automated analysis. Log monitoring consoles are utilized to generate reports.

The Division of Enterprise Technology (DET) has implemented these tiers as follows:

- Tier 1 (Log Generation)—Most server environments are generating logs.
- Tier 2 (Log Analysis and Storage)—About 20% of servers hosted by DET are transmitting logs to the existing central log service storage environment.
- Tier 3 (Log Monitoring)—Aside from manual analysis, DET has a four year old MARS appliance for log analysis and monitoring.

Agencies that have some level of centralized logging implemented include Workforce Services, Public Safety, and Alcohol and Beverage Control. Most log analysis and monitoring is somewhat limited. Health and Tax have some limited logging. All of these agencies have substantial gaps in log analysis and monitoring. ABC has an effective system for log creation, analysis, and monitoring.

Emerging Technologies and Industry Trends

The industry is migrating toward Security Information and Event Management (SIEM) solutions. They are a combination of the formerly disparate product categories of SIM (Security Information Management) and SEM (Security Event Management). SIEM technology provides real-time analysis of security alerts generated by network hardware and applications. The objective is to help companies respond to attacks faster and organize mountains of log data. SIEM solutions come as software, appliances, or managed services. Increasingly, SIEM solutions are being used to log security data and generate reports for compliance purposes.

In 2006, IBM, Novell, and EMC bought their way into the SIEM market, leaving Arcsight, with its Enterprise Security Manager product, as the current market leader. Network Intelligence, which EMC acquired in September, previously occupied that spot on the strength of its enVision product, used by many Managed Security Service Providers (MSSPs) to deliver SIEM-as-a-service. IBM acquired Consul and Micromuse, and Novell bought e-Security to get into this space. In addition, Attachmate acquired NetIQ.

Cisco's MARS appliance, which is currently used in DET, is sometimes seen as a SIEM product. Solution providers said it focuses mainly on the event management portion of SIEM as opposed to logging data for forensics purposes.

The top providers in the SIEM market include:

- Arcsight—Enterprise Security Manager
- EMC/Network Intelligence—Envision
- IBM/Consul—Micromuse
- Novell—eSecurity
- Attachmate—NetIQ
- Cisco—MARS

Other SIEM vendors and their products include:

- Check Point—Eventia
- LogLogic—ST and LX Appliances
- eIQ Networks—SecureVue
- CA (NYSE:CA)—eTrust Security Command Center
- Symantec (NSDQ:SYMC)—SIM appliance
- SenSage—Enterprise Security Analytics (ESA)
- Q1 Labs—Qradar

Other major providers[2] that are not listed as SIEM solutions, but have a dominant market share for logging, include Log Logic, Snare, and Splunk. These applications are widely used with government agencies that have to deal with various types of regulatory compliance.

Financial Analysis

This area represents a needed investment by DTS Security. Logging and analysis is a best practice for security and is a legal requirement for a number of State agencies, so this requires attention and investment beyond current levels. These kinds of services can be funded with existing security rates, new rate and subscription approaches, direct appropriation, or a combination of funding methods.

Tools for analysis and monitoring are costly and are best provided as a centralized service. Failure to do so will encourage redundant investments among those agencies that must meet legally mandated logging requirements.

Security Review and Analysis

Failure to provide adequate monitoring and analysis places the State in a highly reactive mode with regards to security breaches and events. Security must have the opportunity to aggregate events and alerts from one agency and consider impacts on the enterprise. Effective logging, monitoring, and analysis help make that possible.

Operational and Infrastructure Analysis

A much higher percentage of servers must generate logs and transmit either the logs or, in the case of remote locations, events and alerts to a central logging environment. This will require an investment in software tools, training, and the addition of many additional servers to a centralized logging environment. As agencies continue to move server environments to State data centers, some review of the security models that are required by applications is essential, especially for specialized logging and monitoring requirements.

[2] Enterprise log management - a comparison of 3 big logging systems (Snare vs. Splunk vs. LogLogic) at http://www.tweako.com/enterprise_log_management_a_comparison_of_3_big_logging_systems_snare_vs_splunk_vs_loglogic

Solution Delivery Impact and Analysis

There is minimal impact on solution delivery, however, logging requirements must be considered and addressed for all new, upgraded, and currently maintained applications.

Agency Services Impact and Analysis

Agency service impact is positive if DTS supports agency logging and monitoring requirements. Failure to do so has the potential for imposing additional duplicative costs on agencies, and could make it more difficult for agencies to meet the logging and security requirements of external entities such as the federal government.

Summary and Recommendations

Centralized logging services, including monitoring and analysis, are a prime area for providing value added enterprise services to agencies. DTS has an opportunity to provide analysis and monitoring services for all agencies. There are substantial gaps in the number of servers and applications that are currently monitored, and existing logging and analysis infrastructure is becoming dated. DTS should consider:

- developing a product definition and scope for logging services;
- defining the funding mechanisms for supporting centralized logging services at the least cost to agencies;
- assessing the existing server population to identify what servers should be added to centralized logging pools;
- meeting with agencies and documenting specific logging requirements, including those required by law or rule from other entities such as the federal government;
- establishing processes to integrate alerts and events from agencies that are doing centralized logging so they can be integrated with other enterprise alerts and events;
- updating the existing DET central logging environment with the objective of providing additional services to agencies that have specific logging requirements; and,
- releasing a competitive RFP for the procurement of SIEM software or appliances for enterprise logging services analysis and monitoring and procure needed infrastructure.

Centralized logging services require additional investment to be effective. Failure to invest on an enterprise level pushes added expense to agencies, which should be avoided. Effective SIEM tools are costly, but those costs can be more easily leveraged across the State than by any single agency. These services represent a substantial opportunity for DTS to add value to existing agency business needs.

References

Allred, Michael, *Business Case: Logging Analyzer and Monitoring Device,* DET, April 25, 2005

_____*, System Logging and Monitoring Policy (Draft Document),* Department of Technology Services [No Date]

_____*, Vision and Scope: Centralized Logging Server,* Information Technology Services, July 9, 2004*.*

Enterprise log management - a comparison of 3 big logging systems (Snare vs. Splunk vs. LogLogic) at http://www.tweako.com/enterprise_log_management_a_comparison_of_3_big_logging_systems_snare_vs_splunk_vs_loglogic

Guide to Computer Security Log Management, NIST Special Publication (SP) 800-92, September 2006.

Recommended Security Controls for Federal Information Systems, NIST Special Publication (SP) 800-53.

Tax Information Security Guidelines for Federal, State and Local Agencies and Entities: Safeguards for Protecting Federal Tax Returns and Return Information, IRS Publication 1075, February 2007.